

IN THE CLAIMS

1 - 16. (canceled)

17. (new) A method of access control to a secure area comprising:

obtaining a first biometric reading at a first station from a person seeking access to the secure area;

recording said first biometric reading on a card as biometric data;

providing a means for reading the biometric data on said card at a second station located at the secure area;

obtaining a second biometric reading from the person; and

comparing the biometric data on the card with the second biometric reading to ensure that the person giving the second biometric reading is the same person giving the first biometric reading.

18. (new) the method according to claim 17, wherein the card having biometric data is returned to the person after obtaining the first biometric reading.

19. (new) The method according to claim 17, wherein the card having biometric data is retained by a security personnel.

20. (new) The method according to claim 17, wherein a non-graphic method is used to compare the second biometric reading with the biometric data recorded on the card.

21. (new) The method according to claim 17, wherein the card comprises a magnetic strip and a memory means for recording the biometric data on the magnetic strip of the card.

22. (new) The method according to claim 17, wherein an identity document is used to conduct an identity check on the person at the same time the biometric reading is obtained from the person.

23. (new) The method according to claim 17, further comprising using a computing means to compare said first and second biometric readings.

24. (new) The method according to claim 17, wherein the biometric data comprises at least one fingerprint of the person.

25. (new) The method according to claim 17, wherein the biometric data comprises data about the eye of the person.

26. (new) The method according to claim 17, wherein the biometric data comprises data about voice parameters of the person.

27. (new) The method according to claim 17, wherein the biometric data comprises geometric parameters of the face of the person.

28. (new) The method according to claim 17, wherein the biometric data comprises geometric parameters of the person's hand.

29. (new) The method according to claim 17, wherein the card is a supple boarding pass.

30. (new) The method according to claim 29, wherein the card is comprised of a material that can be torn off by the person, so that the person may easily destroy the biometric data on the card.

31. (new) The method according to claim 17, wherein the card is comprised of a plastic material.

32. (new) The method according to claim 17, wherein the second station comprises a check-in desk provided with routing means of routing luggage to the secure area; automatic means for obtaining a second biometric reading from a person; and means for recording the second biometric reading on a card as comparison biometric data, so that the first biometric reading is conducted at the same time as the person's luggage is checked in.

33. (new) The method according to claim 17, wherein the second station includes an access gate to the secure area, a reading desk comprising a module for automatically reading biometric data written on the card of the person wishing to

access the secure area, a biometric sensor, and means for automatically comparing the second biometric reading recorded by the sensor on the person with biometric data written on the card.

34. (new) A module for an automatic access control to a transport vehicle, comprising:

reading means for automatically reading data recorded on an access card, the reading means reading biometric data recorded on the access card in the form of text;

a sensor for sampling biometric data on a person; and

comparison means for automatically comparing biometric data on the card with data recorded by the sensor, the comparison means capable of indicating that data on the access card and data provided by the sensor belong to a same person.

35. (new) An access control assembly for permitting access to a secure area, comprising:

writing means for writing data onto a card controlling access to the secure area at a first site, and

reading means for automatically reading the card at a second site,

the writing means including a first sensor for sampling biometric data on a person, and

the reading means including automatic means for reading biometric data written on the cards; a second sensor for sampling biometric data from a person; and comparison means for making an automatic comparison between the biometric data read on the card and the data read by the sensor, the comparison means capable of indicating if the data on the card and the data on the sensor belong to the same person.

36. (new) The assembly according to claim 35 wherein the writing means at the first site is at least a partially non-graphic method.